RECEIVED
CENTRAL FAX CENTER
JUN 13 2006

ZILKA-KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	June 13, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P055/01.228.01 **App. No: 10/028,651**

Total Number of Pages Being Transmitted, Including Cover Sheet: 26

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

****
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.
****

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

PAGE 1/26 * RCVD AT 6/13/2006 7:00:36 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):05-06

RECEIVED
CENTRAL FAX CENTER

JUN 13 2006

Practitioner's Docket No. NAI1P055/01.228.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lee Codel Lawson Tarbotton et al

Application No.: 10/028,651 Group No.: 2137
Filed: 12/20/2001 Examiner: Pyzocha, M.
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR PRECLUDING WRITES TO CRITICAL FILES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on March 13, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

06/14/2006 TL0111 00000021 501351 10028651
01 FC:1402 500.00 DA
02 FC:1251 120.00 DA

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

*(When using Express Mail, the Express Mail label number is **mandatory**; Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ _ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 6/13/2006

Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

PAGE 2/26 * RCVD AT 6/13/2006 7:00:36 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):05-06

RECEIVED
CENTRAL FAX CENTER

JUN 13 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:
other than a small entity $500.00

Appeal Brief fee due **$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for one month:
Fee: $120.00

If an additional extension of time is required, please consider this a petition therefor.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:
Appeal brief fee $500.00
Extension fee (if any) $120.00

TOTAL FEE DUE **$620.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $620.00 to Deposit Account No. 50-1351 (Order No. NAI1P055).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P055).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PAGE 3/26 * RCVD AT 6/13/2006 7:00:36 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):05-06

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Tarbotton et al.	Group Art Unit: 2137
Application No. 10/028,651	Examiner: Pyzocha, Michael J.
Filed: 12/20/2001	Date: 06/13/2006
For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR PRECLUDING WRITES TO CRITICAL FILES	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 03/13/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI ISSUES
VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE APPEAL

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, below is a list of such appeals, interferences, or related judicial proceedings.

No such pending appeals, interferences, or related judicial proceedings exist.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-10, 12-23, 25-28, and 30-31

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-10, 12-23, 25-28, and 30-31
3. Claims allowed: None
4. Claims rejected: 1-10, 12-23, 25-28, and 30-31
5. Claims cancelled: 11, 24, and 29

C. CLAIMS ON APPEAL

The claims on appeal are: 1-10, 12-23, 25-28, and 30-31

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there is no amendment after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1, 14, and 27, as shown in Figures 1-5, a method, computer program product, and system are provided for preventing writes to critical files. In operation, factors associated with a computer are identified (e.g. see page 4, line 4, etc.). Further, requests to write files on the computer are monitored (e.g. see page 4, lines 4-5, etc.). As shown in item 500 of Figure 5, writes to the files on the computer are prevented based on the factors to prevent virus proliferation (e.g. see page 10, lines 21-26, etc.). The factors are altered based on the monitoring of the requests to write to the files on the computer. Additionally, the factors are updated based on the requests (e.g. see page 10, lines 24-26, etc.).

With respect to a summary of Claim 28, as shown in Figures 1-5, a method is provided for preventing writes to critical files by identifying an operating system associated with the computer (e.g. see item 301 of Figure 3, etc.). Further, at least one of the critical files and critical file locations associated with the operating system are looked up (e.g. see item 302 of Figure 3, etc.). Also, access to the at least one of the critical files (e.g. see item 514 of Figure 5, etc.) and critical file locations (e.g. see item 502 of Figure 5, etc.) associated with the operating system are prevented to prevent virus proliferation (e.g. see page 11, line 6-page 12, line 14 et al., etc.). In addition, the at least one of critical files and critical file locations are looked up based on requests to write to the at least one of critical files and critical file locations on the computer.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-7, 9-10, 12-20, 22-23, 25-28, and 30-31 under 35 U.S.C. 103(a) as being unpatentable over "Q222193- Description of the Windows 2000 Windows File Protection Feature" (hereinafter WFP), in view of Rickey et al. (U.S. Publication No. 2002/0166059).

Issue # 2: The Examiner has rejected Claims 8, and 21 under 35 U.S.C. 103(a) as being unpatentable over WFP, in view of Rickey et al., in view of Stevens (U.S. Publication No. 2002/0133702).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-7, 9-10, 12-20, 22-23, 25-28, and 30-31 under 35 U.S.C. 103(a) as being unpatentable over "Q222193- Description of the Windows 2000 Windows File Protection Feature" (hereinafter WFP), in view of Rickey et al. (U.S. Publication No. 2002/0166059).

Group #1: Claims 1-2, 4-7, 13-15, 17-20, and 26-27

With respect to the current grouping, and specifically appellant's claimed technique "wherein the factors are altered based on the monitoring of the requests to write to the files on the computer," the Examiner has responded to appellant's arguments by stating that "when WFP is monitoring for modifications to files the write request is part of the change and therefore part of the monitoring." First, appellant respectfully asserts that what is claimed is "factors [that] are altered based on the monitoring of the requests" (emphasis added), and not merely monitoring write requests, as the Examiner has argued. Appellant emphasizes that WFP teaches that the "Windows File Protection feature is implemented when it is notified that a file in a protected folder is modified" and that a "second protection mechanism [is]...the System File Checker tool [that] scans all protected files to ensure they are not modified." Thus, WFP only discloses a situation where it is determined if a file has already been modified, and not altering factors "based on the monitoring of the requests," as claimed by appellant (emphasis added). Furthermore, WFP discloses restoring a file to a correct Microsoft version, but not altering factors associated with the computer, in the manner claimed by appellant.

Second, appellant respectfully disagrees with the Examiner's argument that "each time a file [is] written (i.e. modified) a write request occurs" such that "the write request [which is] part of the change... [is] therefore part of the monitoring." Specifically, WFP only teaches that the

"Windows File Protection feature is implemented when it is notified that a file in a protected folder is modified" and that "[o]nce the notification is received, the Windows File Protection feature determines which file was changed" (emphasis added). Thus, in WFP, the monitoring is performed with respect to when an actual modification has already been made, and not to when a request to write to the files on the computer is made, in the manner claimed by appellant. To emphasize, appellant claims altering factors based on a request, and not merely a file modification that has already been made, as in WFP. As such, appellant's claim language allows for the "writes to the files on the computer" to be prevented such that the modification is not made.

Still with respect to the present grouping, and specifically appellant's claimed technique "wherein the factors are updated based on the requests," the Examiner has responded to appellant's arguments by stating that in WFP "when a file is changed to an incorrect version, WFP replaces the file with the correct version, which is both altering and updating." Appellant respectfully asserts that WFP only teaches responding to the actual modifications of files, and not to "update[ing] based on the requests," as claimed by appellant (emphasis added). In addition, appellant claims that "the factors are updated" (emphasis added), and not merely that the file is replaced, as in WFP.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 28

With respect to the present grouping, the Examiner relied upon pages 1-2 in WFP to make a prior art showing of appellant's claimed technique "wherein the at least one of critical files and critical file locations are looked up based on requests to write to the at least one of critical files and critical file locations on the computer." Appellant respectfully asserts that pages 1-2 from WFP merely teach "cache[ing] all protected system files" in order to replace any modified protected files. However, restoring protected system files from a cache or installation media after they are modified clearly fails to even suggest a technique "wherein the at least one of critical files and critical file locations are looked up based on requests to write to the at least one of critical files and critical file locations on the computer" (emphasis added), as claimed by appellant.

Group #3: Claims 3 and 16

With respect to the present grouping, the Examiner has relied on page 2 in WFP to make a prior art showing of appellant's claimed technique "wherein the factors are user configurable." Appellant respectfully asserts that the only mention of users in the excerpt from WFP only discloses that an "administrator [has] the ability to scan all protected files to verify their versions" and that an "administrator [is prompted] to insert the appropriate media to replace the file." Clearly, neither teaching even suggests user configurable factors, in the manner claimed by appellant.

In the Office Action mailed 01/12/2006, the Examiner has responded to appellant's arguments by stating that "at the bottom of page 1 WFP teaches that a user can allow a file to be updated and therefore the [user] configures a factor." Appellant respectfully disagrees. The bottom of page 1 in WFP only discloses that the Windows File Protection feature is notified of a file modification and that the Windows File Protection feature looks up the file signature in a catalog to determine if a new file is the correct Microsoft version. Thus, in WFP, only the Windows File Protection feature allows files to be updated, which clearly does not meet appellant's claimed "factors [that] are user configurable" (emphasis added). Appellant also notes that the only mention of users in WFP discloses that an "administrator [has] the ability to scan all protected files to verify their versions" and that an "administrator [is prompted] to insert the appropriate media to replace the file." Clearly, neither teaching even suggests user configurable factors, in the manner claimed by appellant.

Group #4: Claims 9, 10, 22, and 23

With respect to the present grouping, the Examiner has again relied on pages 2-3 in WFP to make a prior art showing of appellant's claimed techniques "wherein the factors are updated based on a user request" (Claim 9 et al.) and "wherein the factors are updated from a remote location via a network" (Claim 10 et al.). Appellant respectfully asserts that WFP only teaches responding to modifications of files, and not to requests, as claimed by appellant (Claim 9 et. al.). In addition, WFP fails to even mention any sort of updating, and especially not updating factors, as claimed by appellant (Claims 9 and 10 et al.), but instead only discloses repairing incorrect file versions.

In the Office Action mailed 01/12/2006, the Examiner has responded to appellant's arguments by stating that "when a file is changed to an incorrect version, WFP replaces the file with the correct version, which is both altering and updating." Appellant again respectfully asserts that WFP only teaches responding to the actual modifications of files, and not to requests, as claimed by appellant (Claim 9 et. al.). In addition, WFP fails to even mention updating factors, as claimed by appellant (Claims 9 and 10 et al.), but instead only discloses replacing files.

Group #5: Claims 12 and 25

With respect to the present grouping, the Examiner relied on the bottom of page 2 in WFP to make a prior art showing of appellant's claimed technique for "conditionally preventing the writes to the files on the computer based on a user confirmation." Appellant respectfully asserts that the excerpt from WFP relied upon by the Examiner merely teaches that "if the affected file in use by the operating system is not the correct version or the file is not cached in the Dllcache folder, the Windows File Protection feature attempts to locate the installation media." WFP continues by teaching that "[i]f the installation media is not found, the Windows File Protection feature prompts an administrator to insert the appropriate media to replace the file or the Dllcache file version" (emphasis added). Clearly, suggesting to prompt an administrator to insert media in order replace the file or Dllcache file fails to even suggest a technique for

"conditionally preventing the writes to the files on the computer based on a user confirmation" (emphasis added), as claimed by appellant.

Group #6: Claim 30

With respect to the present grouping, the Examiner relied on page 2 in WFP to make a prior art showing of appellant's claimed technique "wherein the factors include a list of critical files such that the list of critical files is updated based on the requests." Appellant respectfully asserts that page 2 in WFP teaches that "[a]ll SYS, DLL, EXE, TTF, FON and OCX files included on the Windows 2000 CD-ROM are protected" and that "[s]etting the SFCQuota value to 0xFFFFFFFF causes the Windows File Protection feature to cache all protected system files (approximately 2,700 files)." Clearly, disclosing that all SYS, DLL, EXE, TTF, FON and OCX files are protected and that the SFCQutoa value determines the size of the Dllcache folder simply fails to even suggest a technique "wherein the factors include a list of critical files such that the list of critical files is updated **based on the requests**" (emphasis added), as claimed by appellant.

Group #7: Claim 31

With respect to the present grouping, the Examiner relied on page 1 in WFP to make a prior art showing of appellant's claimed technique "wherein if one of the requests is initiated by an application that is not one of the trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application." Appellant respectfully asserts that page 1 from WFP discloses that "[t]he Windows File Protection feature provides protection for the system files using two mechanisms." WFP teaches that the first mechanism of "[t]he Windows File Protection feature is implemented when it is notified that a file in a protected folder is modified." Clearly, the excerpt from WFP fails to even suggest a technique "wherein if one of the requests is initiated by an application that is not one of the trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application" (emphasis added), as claimed by appellant. Additionally, appellant respectfully asserts that the Windows File Protection feature is invoked only after a file is replaced or deleted, and not before. Thus, WFP fails to suggest that "a user is alerted and allowed to at least one of prevent and permit the request initiated by the application" (emphasis added), as claimed by appellant.

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Issue # 2:

The Examiner has rejected Claims 8, and 21 under 35 U.S.C. 103(a) as being unpatentable over WFP, in view of Rickey et al., in view of Stevens (U.S. Publication No. 2002/0133702). In particular, the Examiner relied upon the following excerpt from Stevens to make a prior art showing of appellant's claimed technique "wherein the factors include trusted applications that initiate the requests."

> "The above five functions implemented by the present invention allow the system firmware (BIOS) to determine that a trusted application is attempting access and then to grant the requested access." (Stevens, Paragraph 0019 - emphasis added)

Appellant respectfully asserts that the excerpt from Stevens merely discloses to "allow the system firmware (BIOS) to determine that a trusted application is attempting access and then to grant the requested access" (emphasis added). Clearly, the system firmware granting requested access when the system firmware determines that a trusted application is attempting access simply fails to even suggest a technique "wherein the factors include trusted applications that **initiate the requests**" (emphasis added), as claimed by appellant. There simply is no disclosure in the excerpt from Stevens that a trusted application initiates the request, as claimed by appellant.

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for preventing writes to critical files, comprising:
(a) identifying factors associated with a computer;
(b) monitoring requests to write to files on the computer; and
(c) conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;
(d) wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;
(e) wherein the factors are updated based on the requests.

2. (Original) The method as recited in claim 1, wherein the factors are selected from the group consisting of critical files, critical file locations, and trusted applications.

3. (Original) The method as recited in claim 1, wherein the factors are user configurable.

4. (Original) The method as recited in claim 1, wherein the factors are identified in a registry.

5. (Original) The method as recited in claim 2, wherein the factors include critical files associated with an operating system of the computer.

6. (Original) The method as recited in claim 2, wherein the factors include critical file locations associated with an operating system of the computer.

7. (Original) The method as recited in claim 6, wherein the critical file locations include folders.

8. (Original) The method as recited in claim 2, wherein the factors include trusted applications that initiate the requests.

9. (Original) The method as recited in claim 1, wherein the factors are updated based on a user request.

10. (Original) The method as recited in claim 1, wherein the factors are updated from a remote location via a network.

11. (Cancelled)

12. (Original) The method as recited in claim 1, and further comprising conditionally preventing the writes to the files on the computer based on a user confirmation.

13. (Original) The method as recited in claim 12, wherein the factors are updated based on the user confirmation.

14. (Previously Presented) A computer program product for preventing writes to critical files, comprising:

(a) computer code for identifying factors associated with a computer;

(b) computer code for monitoring requests to write to files on the computer; and

(c) computer code for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;

(d) wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;

(e) wherein the factors are updated based on the requests.

15. (Original) The computer program product as recited in claim 14, wherein the factors are selected from the group consisting of critical files, critical file locations, and trusted applications.

16. (Original) The computer program product as recited in claim 14, wherein the factors are user configurable.

17. (Original) The computer program product as recited in claim 14, wherein the factors are identified in a registry.

18. (Original) The computer program product as recited in claim 15, wherein the factors include critical files associated with an operating system of the computer.

19. (Original) The computer program product as recited in claim 15, wherein the factors include critical file locations associated with an operating system of the computer.

20. (Original) The computer program product as recited in claim 19, wherein the critical file locations include folders.

21. (Original) The computer program product as recited in claim 15, wherein the factors include trusted applications that initiate the requests.

22. (Original) The computer program product as recited in claim 14, wherein the factors are updated based on a user request.

23. (Original) The computer program product as recited in claim 14, wherein the factors are updated from a remote location via a network.

24. (Cancelled)

25. (Original) The computer program product as recited in claim 14, and further comprising computer code for conditionally preventing the writes to the files on the computer based on a user confirmation.

26. (Original) The computer program product as recited in claim 25, wherein the factors are updated based on the user confirmation.

27. (Previously Presented) A system for preventing writes to critical files, comprising:

(a) logic for identifying factors associated with a computer;

(b) logic for monitoring requests to write to files on the computer; and

(c) logic for conditionally preventing the writes to the files on the computer based on the factors to prevent virus proliferation;

(d) wherein the factors are altered based on the monitoring of the requests to write to the files on the computer;

(e) wherein the factors are updated based on the requests.

28. (Previously Presented) A method for preventing writes to critical files, comprising:

(a) identifying an operating system associated with a computer;

(b) looking up at least one of critical files and critical file locations associated with the operating system; and

(c) preventing access to the at least one of critical files and critical file locations associated with the operating system to prevent virus proliferation;

(d) wherein the at least one of critical files and critical file locations are looked up based on requests to write to the at least one of critical files and critical file locations on the computer.

29. (Cancelled)

30. (Previously Presented) The method as recited in claim 1, wherein the factors include a list of critical files such that the list of critical files is updated based on the requests.

31. (Previously Presented) The method as recited in claim 8, wherein if one of the requests is initiated by an application that is not one of the trusted applications, a user is alerted and allowed to at least one of prevent and permit the request initiated by the application.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P055).

Respectfully submitted,

By: _____ Date: 6/13/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660